



Ishuff
2131

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of)
Peyravian et al.)
Serial No. 09/458,921) Vaughan, Michael R.
Filed: December 10, 1999) Examiner
For: TIME STAMPING METHOD USING) Group Art Unit 2131
TICKETS AND STUBS) Confirmation No. 9480
Attorney's Docket No. 4541-001)

Raleigh, North Carolina

December 1, 2004

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certificate of Mailing
I hereby certify that this document is being deposited with the United States Postal Service as first class mail on the date indicated below, postage prepaid, in an envelope addressed to: Mail Stop Appeal Brief - Patents, Commissioner for Patents, Box 1450, Alexandria, VA 22313-1450 on December 1, 2004.

Stephen A. Herrera

APPEAL BRIEF

Sir:

The present appeal brief is filed in triplicate pursuant to 37 C.F.R. § 1.192. The Commissioner is hereby authorized to charge the requisite fee under 37 C.F.R. § 1.17(c) to IBM's Deposit Account No. 09/0461.

(1) REAL PARTY IN INTEREST

The real party in interest is IBM Corp., the assignee of the present invention.

(2) RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences to the best of Applicants' knowledge.

(3) STATUS OF CLAIMS

A total of 50 claims have been presented for examination, all of which are pending. Claims 1-50 stand rejected by the Examiner. Accordingly, Applicants appeal the rejection of claims 1-50.

(4) STATUS OF AMENDMENTS

All amendments have been entered to the best of Applicants' knowledge.

(5) SUMMARY OF INVENTION

Applicant's invention relates to a two-step method for generating certified time stamp receipts for digital documents. Spec., pg. 4, ll. 1-6. During the first stage or "ticketing" stage, identifying data such as a hash of the document, is presented to a time stamping authority. Spec., pg. 4, ll. 7-9. The time stamping authority appends a time stamp to the identifying data to create an uncertified time stamp receipt. Additionally, the time stamping authority generates a message authentication code based on the uncertified time stamp receipt and a secret key. Spec., pg. 4, ll. 9-13. The uncertified time stamp receipt and the message authentication code is transmitted to the requestor. Spec., pg. 4, ll. 13-14.

During the second stage or the process, or "certification" stage, a holder of the time stamp receipt and the message authentication code (e.g., the original requestor or other third party) may request certification. The holder presents the uncertified time stamp receipt and the message authentication code to the time stamping authority.

Spec., pg. 4, ll. 15-16. The time stamping authority validates the message authentication code and, if the message authentication code is valid, generates a certified time stamp receipt using, for example, a private signature key. *Spec.*, pg. 4, ll. 17-22. The certified time stamp receipt is then sent back to the holder that requested certification. The certified time stamp receipt serves as proof of the date and time that the document was received at the TSA. *Spec.*, pg. 4, ln. 22 – pg. 5, ln. 2.

(6) ISSUES

The first issue is whether claims 1-14, 29-40, and 41-50 are unpatentable under 35 U.S.C. §103(a) over the patent to Haber et. al., (U.S. Patent No. RE 34, 954, hereinafter “Haber”) in view of the book entitled “Applied Cryptography” authored by Schneier (hereinafter “Schneier”).

The second issue is whether claims 15-28 are unpatentable under 35 U.S.C. §103(a) over Haber et. al., in view of Schneier, and in further view of the patent to Doyle (WO 99/16209, hereinafter “Doyle”).

The third issue is whether claims 29-40 are unpatentable under 35 U.S.C. §103(a) over the patent to Haber in view of the book of Schneier.

The fourth issue is whether claims 41-50 are unpatentable under 35 U.S.C. §103(a) over the patent to Haber in view of the book of Schneier.

(7) GROUPING OF CLAIMS

Group I: Claims 1-14.

Group II: Claims 15-28.

Group III: Claims 29-40.

Group IV: Claims 41-50.

All claims in each group stand or fall together.

(8) ARGUMENT

A. A SUMMARY OF THE CITED REFERENCES

The Examiner rejected claims 1-14, 29-36, and 41-48 under 35 U.S.C. §103(a) over Haber in view of Schneier. The Examiner also rejected claims 15-28, 37-40, and 49-50 under 35 U.S.C. §103(a) over Haber in view of Schneier and in further view of Doyle.

Haber discloses a method for securely time-stamping a digital document received at a trusted agency. In Haber, a document author sends a hash of a digital document to the trusted agency. Upon receipt, the trusted agency time stamps the received hash value, cryptographically signs the time stamp, and returns the certified time stamp receipt to the document author. *Haber*, col. 2, ln. 66 – col. 3, ln. 10. Importantly, however, the method of Haber is specifically intended to prevent any possible collusion between the author of the document being time stamped and the trusted agency. *E.g., Haber*, col. 2, ll. 38-54; col. 3, ll. 57-65. Thus, Haber discloses two embodiments to ensure the validity of the time stamp. *E.g., Haber*, col. 4, ll. 5-7.

In the first embodiment, the trusted agency generates a “composite” time stamp receipt that includes time stamp data for the current document as well as for documents received both before and after the current document. The data includes, for example, the time of receipt, the hash value, and the author ID. This “fixes” the current document in a continuum of time, and ensures against collusion. Particularly, each author having information in the composite time stamp receipt receives a copy of the composite time stamp receipt from the trusted agency. Any author wishing to alter his own time stamp information must also contend with multiple copies distributed to multiple authors. Any later comparison would quickly reveal a discrepancy. *Haber*, col. 4, ll. 8-38.

In the second embodiment, the disclosed method relies on a presumption that at least some members of the trusted agency will not participate in collusion. Particularly,

the trusted authority distributes the task of time stamping the document to a number of randomly selected “agents.” The agents may be, for example, authors or other independent parties that utilize the time stamp service. The agents each generate a time stamp receipt for the document using the method described above, and returns the time stamp receipts to the author or the trusted agency. The randomness removes the possibility that any given author could pick and choose an agent willing to participate in collusion. *Haber*, col. 4, ln. 39 – col. 5, ln. 21.

The Schneier reference is a book written by Bruce Schneier. It provides a basic introduction into the field of crytology, and provides information regarding one-way hash functions, Message Authentication Codes (MACs), and public-key algorithms. *E.g.*, *Schneier*, pp. 30-31, and 455-459. In essence, the information in Schneier discloses what these aspects of crytology are and broadly how they might be used.

Doyle also discloses a method of time stamping digital documents such that the veracity of their time stamp is unquestionable. *Doyle*, pg. 6, ll. 10-16. In one embodiment, the system of Doyle generates unique public/private key pairs during specified time intervals (e.g., every second). The private key is used to digitally sign a document during the specified time period, and then permanently destroyed. The public key is archived for later use in certifying the document. If no documents require signing during the specified time period (e.g., one second), then the pair is destroyed and a new pair is generated. *Doyle*, Figure 1; p. 8, ln. 31 – pg. 10, ln. 23.

In another embodiment, Doyle teaches that public/private keys pairs are generated for successive time intervals t_n , t_{n+1} . The private key generated during interval t_n is used to sign the public key generated during interval t_{n+1} , and then permanently deleted. The public key generated during interval t_n is then archived. Any documents requiring time stamping during interval t_{n+1} are signed using the private key t_{n+1} . During verification, the public key t_{n+1} must be used to authenticate the document signature.

However, the public key t_{n+1} is itself signed with the private key t_n . Thus, the public key t_{n+1} needed to authenticate the signature of the document must first be authenticated using the public key t_n . *Doyle*, pg. 10, ln. 25 – pg. 13, ln. 23. According to Doyle, this method ensures validity without having to rely on a trusted institution or other administrating official. *Doyle*, pg. 6, ln. 10-16.

B. THE EXAMINER HAS FAILED TO PUT FORTH A LEGALLY SUFFICIENT PRIMA FACIE CASE OF OBVIOUSNESS.

1. GROUP I

Claim 1, the independent claim of Group 1, relates to a two-stage process in which a Time Stamping Authority (TSA) receives a time stamp request at a first time, and a certification request at a second time. The TSA generates and later certifies both the time stamp receipt and the message authentication code. Notably, generation of the message authentication code of claim 1 is based on the generated time stamp receipt and a secret key. For convenience, claim 1 appears below.

1. A method for time stamping a document comprising:
 - a. receiving a time stamp request at an outside agency at a first time, said time stamp request including identifying data associated with said document;
 - b. creating at said outside agency a time stamp receipt based on said identifying data and a time indication; and
 - c. generating at said outside agency a message authentication code based on said time stamp receipt and a secret key;
 - d. transmitting said time stamp receipt and said message authentication code to a designated party;
 - e. receiving a certification request at said outside agency at a second time, said certification request including said time stamp receipt and said message authentication code;
 - f. validating said message authentication code at said outside agency using said secret key; and
 - g. certifying said time stamp receipt at said outside agency using a cryptographic signature scheme if said message authentication code is valid.

The Examiner rejected claim 1 under § 103(a) over Haber in view of Schneier. When establishing a *prima facie* case of obviousness, the Examiner has the initial burden to show, *inter alia*, that the cited references teach or suggest all the claim limitations. *MPEP*, §2142. However, neither Haber nor Schneier teach or suggest all the limitations of claim 1, whether taken alone, or in combination.

Specifically, the Examiner admits that Haber fails to teach, “generating at said outside agency a message authentication code based on said time stamp receipt and a secret key,” but falls to Schneier in an attempt to correct the deficiency. However, Schneier teaches nothing of the sort. Schneier is an introductory text on cryptography that simply describes what a MAC is. There is nothing in Schneier that discusses – explicitly or implicitly – that MACs may be used in two-stage time stamping procedures. In fact, Schneier never discusses time-stamping techniques at all. It simply teaches that MACs exist and have utility. Schneier, like Haber, fails to disclose “generating at said outside agency a message authentication code based on said time stamp receipt and a secret key” as recited in claim 1, and moreover, the Examiner never asserts that it does. Thus, neither reference teaches or suggests, alone or in combination, all the claim limitations in claim 1. As such, the § 103 rejection necessarily fails for this reason alone.

Notwithstanding the above facts, however, the §103 rejection also fails for a second reason. Particularly, the Examiner also bears the burden of showing some objective teaching in the prior art, or knowledge generally available to one of ordinary skill in the art that would motivate one to combine the relevant teachings of the references. *In re Fine*, 837 F.2d 1071, 1074, 5 U.S.P.Q.2d 1596 (Fed. Cir. 1988). See also *MPEP*, §2142. Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination. *ACS Hosp. Sys., Inc. v. Montefiore Hosp.*, 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed. Cir. 1984). The combination of elements, in a manner

that reconstructs the applicant's invention only with the benefit of hindsight, is insufficient to establish a *prima facie* case of obviousness. That knowledge cannot come from the applicant's invention itself. *In re Oetiker*, 977 F.2d 1443, 24 U.S.P.Q.2d 1443 (Fed. Cir. 1992).

The question of motivation in this case is similar to the issue of what constitutes a legally sufficient motivation as presented in *ACS Hospital Systems, Inc. v. Montefiore Hospital*, 732 F.2d 1572, 221 U.S.P.Q. 929 (Fed. Cir. 1984). In *ACS Hospital*, the invention related to a television rental system having override switch means. The district court noted that override switches were commonly used, and held the patent invalid under §103. However, despite the apparent widespread use of override switches, the Federal Circuit reversed the district court and concluded that "the trial court's heavy reliance on the widespread use of override switches appears to be no more than hindsight reconstruction of the claimed invention. The court below identified no source, other than the ... patent itself, for the suggestion to use override switching means in a television rental system." *ACS Hospital Systems, Inc. v. Montefiore Hospital*, 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984).

In the instant case, the Examiner cites Schneier merely to show that MACs are well known, and reasons that because of this, have many uses. The Examiner then enumerates the various advantages of using message authentication codes, and uses this reasoning as a basis for supporting an alleged motivation as to why one skilled in the art would combine Schneier with Haber. *Final Office Action*, pp. 5-6. This reasoning is unsubstantiated by the references, and falls far short of the *legally sufficient* reasoning required by the law. The Examiner fails to cite any source to show that message authentication codes are used in time stamping procedures, and simply relies on Schneier to show that MACs exist and have many known uses. However, as evidenced by *ACS Hospital*, the mere fact that MACs may exist and be in widespread use, as the

Examiner contends, means nothing with respect to patentability. While Schneier may disclose some uses for MACs, not one teaches or suggests that a MAC may be used in time stamping procedures at all, let alone two-stage time stamping procedures as recited by claim 1. Therefore, Schneier cannot possibly provide a motivation to combine with Haber.

Haber also fails to provide any motivation to combine with Schneier, although the Examiner contends otherwise. *Final Office Action*, pp. 2-3. The Examiner equates the “one-way function” disclosed in Haber to the requisite MAC. Respectfully, however, this assertion appears based on a misunderstanding of the teachings of Haber. Haber may disclose a use of a one-way function, but it does not disclose the use of a MAC as recited in claim 1. Haber teaches only that a one-way function may be used to create a hash value representative of the document. “By means of the md4 algorithm [i.e., one-way function], the document is hashed ... to a number H_k .” *Haber*, col. 6, ll. 5-6. In a later passage, Haber explicitly reveals that the hash H_k is included in the time stamp receipt along with other information. “The receipt would then comprise the string (r_k, t_k, ID_k, H_k) .” *Haber*, col. 6, ll. 27-28. Thus, Haber only uses the one-way function to create a hash-value that represents the data in the document.

Contrast this with claim 1, which requires generating the MAC based on the time stamp receipt and a secret key. In other words, the TSA in claim 1 receives the request and generates a time stamp receipt. The time stamp receipt includes the data identifying the document (e.g., the hash-value). The MAC is then generated based in part on this time stamp receipt. As such, the one-way function in Haber is employed in a completely different manner than is the MAC of claim 1. Specifically, generating an artifact for inclusion in another is not the same as generating an artifact based on another. One cannot teach or suggest the other.

Additionally, assuming *arguendo* that one could interpret the one-way function of Haber as the Examiner contends, Haber still provides no motivation to combine with Schneier. In particular, Haber shows no need or desire to generate and use a MAC as the Examiner asserts. According to Haber,

[c]onfirmation of the signature at a later time, such as by decryption with the TSA's public key, proves to the author and to the universe at large that the certificate originated with the TSA. Proof of the veracity of the time-stamp itself, however, relies upon a following additional aspect of the invention.

Haber, col. 4, ll. 1-7 (emphasis added). Haber discloses this all-important "relied upon" aspect of the disclosed invention immediately following the above-cited passage.

Specifically, Haber discloses two different embodiments. The first embodiment requires generating a time stamp receipt for a given document such that it becomes what Haber refers to as a composite receipt "fixed in the continuum of time." According to Haber, each generated time stamp receipt includes time stamp information for the document being time stamped, and for documents received both before and after the document being time stamped. In other words, the time stamp receipt for each document is necessarily linked in time to other contemporary time stamp receipts. Because the time stamp receipts are distributed to multiple authors, any later comparison of a number of these time stamp receipts would easily reveal a discrepancy. *Haber*, col. 4, ll. 8-38. Haber explicitly extols the virtues of this embodiment stating, "[s]o effective is such a sequential fixing of a document in the [time] stream that the TSA signature could be superfluous in actual practice." *Haber*, col. 4, ll. 36-38.

In the second embodiment, Haber teaches distributing the time stamping task to a plurality of independent agents. A process over which an author has no control randomly selects the number and identity of the selected agents. Once selected, the independent agents may perform the time stamping task and return the time stamp receipts directly to the author. This embodiment eliminates the TSA, or at the least,

reduces its participation to that of an administrative entity. *Haber*, col. 4, ln. 39 – col. 5, ln. 21. Haber is no less clear in proclaiming the advantages of this second embodiment. “The resulting lack of a capability on the part of the author to select a prospective collusive agent of the author’s own choosing substantially *removes the feasibility* of intentional time falsification.” *Haber*, col. 4, ll. 46-58.

Motivation, as articulated by the Federal Circuit, requires that there be some desirability or advantage gained in making the combination, and further, that desirability or advantage must be apparent to one skilled in the art. “The mere fact that the prior art could be so modified would not have made the modification obvious unless the prior art suggested the desirability of the modification.” *In re Gordon* 733 F.2d 900, 902, 221 U.S.P.Q. 1125 (Fed. Cir. 1984) (emphasis added). Indeed, the above passages evidence the fact that Haber shows no need or desire to use a MAC as recited by claim 1. Haber believes to have invented a virtually foolproof method of time stamping documents, and provides no indication whatsoever that using a MAC as recited by claim 1 would make the disclosed method any better or more secure despite the Examiner’s allegations otherwise. *E.g., Final Office Action*, p. 4, ¶3. The Examiner asserts that using the MAC of Schneier in the method of Haber would allow a party to “interact with the trusted agency first hand,” and provide the party with a “second source of validation.” However, neither reference supports the allegation that “first-hand interaction” or “second validation sources” are needed or desired. Applicants note that even the Office Actions are conspicuously devoid of any proof that the cited references teach or suggest this theory. If anything is to be believed with respect to what Haber teaches, it is the fact that Haber does not need to use a MAC as recited by claim 1.

In light of this, the Board must question where the Examiner finds an alleged motivation to combine Haber and Schneier. It did not come from Haber, and as previously stated, Schneier never says anything regarding time stamping methods. The

Examiner provides only an unsubstantiated articulation. The alleged motivation to combine could only have come from Applicants' own disclosure.

Simply put, neither Haber nor Schneier, alone or in combination, teach or suggest the use of a MAC as recited by claim 1. Neither reference teaches or suggests each limitation of claim 1. Further, neither reference supports the Examiner's reasoning on which the alleged motivation is based. Absent the Examiner's unsupported assertions, the Office Action is conspicuously devoid of any proof that shows MACs are used in time stamping procedures as recited in claim 1. The Examiner's enumerated advantages regarding the use of message authentication codes are not something that the Examiner derived from the prior art, but rather, are advantages that could only have been gleaned after reviewing Applicants' application. This is classical hindsight reconstruction, which the Federal Circuit has found time and again to be improper as a *matter of law*. Accordingly, the §103 rejection to claim 1 must fail.

2. GROUP II

The Examiner also rejected claim 15 under §103(a) over Haber in view of Schneier and in further view of Doyle. Claim 15, the independent claim of Group II, is similar to claim 1 in that claim 15 also relates to a two-stage time stamping process. However, claim 15 additionally recites generating first and second message authentication codes, and the use of three secret keys. The first message authentication code is generated based on the time stamp receipt and the first secret key, while the second message authentication code is generated based on the first message authentication code and the first secret key, and signed with a third secret key. The second secret key is used to sign the first secret key to create a key message. The TSA then sends the first and second generated message authentication codes and the key message to whomever requested the time stamp receipt. Upon receiving a certification

request, the TSA validates each of these generated artifacts before it can certify the time stamp receipt as valid. For convenience, claim 15 appears below.

15. A method for time stamping a document comprising:
 - a. receiving a time stamp request at an outside agency at a first time, said time stamp request including identifying data associated with said document;
 - b. creating at said outside agency a time stamp receipt based on said identifying data and a time indication;
 - c. generating at said outside agency a message authentication code based on said time stamp receipt and a first secret key;
 - d. encrypting the first secret key with a second secret key to generate a key message;
 - e. generating a second message authentication code based on said first message authentication code and said first secret key using a third secret key;
 - f. transmitting said time stamp receipt, said first message authentication code, said second message authentication code, and said key message to said requestor;
 - g. receiving at said outside agency at a second time a certification request, said certification request including said time stamp receipt, said first message authentication code, said second message authentication code, and said encrypted key message;
 - h. decrypting at said outside agency said encrypted key message to recover said first secret key;
 - i. validating said second message authentication code at said outside agency using said third secret key;
 - j. validating said first message authentication code at said outside agency using said first secret key if said second message authentication code is valid; and
 - k. certifying said time stamp receipt at said outside agency using a cryptographic signature scheme if said first message authentication code is valid.

In rejecting claim 15, the Examiner first supports the citation of Haber and Schneier with the same reasons as those cited in claim 1. However, for the same reasons stated above with respect to claim 1, Haber and Schneier, alone or in combination, also fail to teach or suggest claim 15. Therefore, the §103 rejection of claim 15 necessarily fails.

In addition, however, the §103 rejection also fails for other reasons. First, none of the references teach or suggest the generation of a second message authentication code based, in part, on a first generated message authentication code. The Examiner

admits that Haber fails to teach or suggest this element, and never asserts that Schneier does. However, the Examiner's assertion that Doyle teaches this element is unsupported and conclusory.

Doyle, like Haber, never teaches generating *any* message authentication codes, let alone first and second message authentication codes. Doyle teaches generating pairs of private/public keys at successive periodic time intervals t_n , t_{n+1} , and using the keys in a specific manner. This includes signing the public key generated during interval t_{n+1} with the private key generated during interval t_n , and signing the *time stamp data* (i.e., the time stamp receipt - not a message authentication code) using the private key generated during interval t_{n+1} . This is clearly evidenced in box 2070 of Figure 2B, which corresponds to the passage cited by the Examiner in supporting the rejection. Doyle never mentions message authentication codes anywhere in the disclosure.

Second, even if the references could somehow be construed to show the second generated message authentication code of claim 15, none of the references discloses signing the second message authentication code using a third secret key as recited in claim 15. More importantly, even the Examiner never asserts that they do. The Examiner rests on Doyle simply to show the generation of multiple secret keys. However, Doyle uses only two. Doyle signs the public key t_{n+1} using the private key t_n , and the time stamp data using the private key t_{n+1} . Thus, there are only *two* private keys employed in Doyle. The requisite third secret key as claimed in claim 15 is never mentioned anywhere other than in Applicants' specification.

Thus, none of the references teach or suggest, alone or in combination, all the elements of claim 15. This is enough of a reason to have the §103 rejection withdrawn. In addition, however, the Examiner has also failed to put forth a *legally sufficient* motivation to combine the references with respect to claim 15. Specifically, the rejection begins with the unsupported theory that Haber and Schneier combined somehow show

generating a first message authentication code based solely upon the notion that MACs are well known and have many uses. This is despite the fact that none of the references disclose using the message authentication codes in time stamping procedures. The Examiner then builds upon this flawed foundation using an overstated, and at times incorrect, characterization of what Doyle actually teaches. However, Doyle simply does not teach or even suggest what the Examiner says it does and in fact, is completely silent on at least some of the requisite aspects of claim 15 (e.g., message authentication codes and a third secret key).

Indeed, it is evident that the reasoning supporting the rejection is speculative at best and unsubstantiated by the references. The only document before the Examiner that recites generating first and second message authentication codes in the manner recited by claim 15 is Applicants' own disclosure. Therefore, the §103 rejection of claim 15 is also based on improper hindsight reconstruction. As such, none of the cited references, alone or in combination teach or suggest claim 15. Accordingly, the §103 rejection of claim 15 must fail.

3. GROUP III

The Examiner rejected claim 29 under § 103(a) over Haber in view of Schneier. Claim 29, the independent claim of Group III, recites an embodiment relates to the phase when the time stamp receipt and message authentication code is generated. For convenience, claim 29 appears below.

29. (Original) A method for time stamping a document comprising:
 - a. receiving a time stamp request at an outside agency at a first time, said time stamp request including identifying data associated with said document;
 - b. creating at said outside agency a time stamp receipt based on said identifying data and a time indication; and
 - c. generating at said outside agency a message authentication code based on said time stamp receipt and a secret key; and
 - d. transmitting said time stamp receipt and said message authentication code to said requestor.

Like claim 1, the message authentication code of claim 29 is generated based on the time stamp receipt and a secret key. In rejecting claim 29, the Examiner simply provides reasons that are similar to, if not the same as, those stated for claim 1. However, as stated above, Haber generates a hash value for inclusion into the time stamp receipt, whereas claim 29 recites generating a value based on the time stamp receipt (that already has a hash value in it). Indeed, these are distinct two concepts – neither of which teach or suggest the other. Moreover, simply because MACs are well known and may have many uses is not a *legally sufficient* reason with which to reject a claim under §103. Thus, for the reasons stated above with respect to claim 1, neither Haber nor Schneier teach or suggest, alone or in combination, claim 29. As such, the §103 rejection to claim 29 must also fail.

4. GROUP IV

The Examiner further rejected claim 41 under § 103(a) over Haber in view of Schneier. Claim 41 is the independent claim of Group IV, and relates to the phase when the time stamp receipt and message authentication code are certified. For convenience, claim 41 appears below.

41. A method for time stamping documents comprising:

- a. receiving at an outside agency a certification request, said certification request including a time stamp receipt and a message authentication code generated on said time stamp receipt;
- b. validating said message authentication code at said outside agency using a secret key;
- c. certifying said time stamp receipt if said message authentication code is valid using a cryptographic signature scheme.

Claim 41 recites that a certification request received at the outside agency must include a time stamp receipt and a message authentication code. However, as stated above, none of the references cited by the Examiner teach or suggest, alone or in combination, generating a message authentication code for use in time stamping

procedures. As such, it necessarily follows that none of the references can teach or suggest, alone or in combination, certifying a time stamp receipt having these elements. Accordingly, the §103 rejection of claim 41 necessarily fails.

In addition, however, Haber explicitly teaches certification of the time stamp receipt is accomplished by applying the same one-way function that was used to originally generate the hash value of the document. Specifically, the certifying party employs the TSA's public key to the time stamp receipt. This reveals the original hash value of the document. The same one-way function used to generate the original hash value (e.g., the md4 function noted above) is then applied to the document itself to generate another hash value. The document is only certified when a comparison of the two hash values results in a match. *Haber*, Abstract, II. 13-22. Contrast this with claim 41, which recites validating the message authentication code using a secret key, and then – provided the message authentication code is valid – certifying the time stamp receipt.

Indeed, claim 41 recites a completely different method than that of Haber. As such, Haber fails to teach or suggest claim 41, and for the reasons stated above with respect to claim 1, Schneier fails to remedy these deficiencies. Therefore, neither Haber nor Schneier, alone or in combination, teach or suggest claim 41, and the §103 rejection must fail.

SUMMARY OF ARGUMENT

The Examiner has failed to establish a *prima facie* case of obviousness. None of the cited references teach or suggest, alone or in combination, each and every element of Applicants' claims. In addition, the motivation to combine the cited references is not based on the cited references themselves, but instead, is based solely on Applicant's own disclosure. This falls far short of the legally sufficient reasoning required by law.

These reasons are enough to warrant the reversal of the §103 rejections.

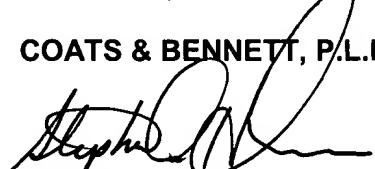
CONCLUSION

For the reasons set forth above, all claims being appealed herein are patentable, and the rejections maintained by the Examiner must be reversed.

Respectfully submitted,

COATS & BENNETT, P.L.L.C.

By:



Stephen A. Herrera
Registration No. 47,642
P.O. Box 5
Raleigh, NC 27602
Telephone: (919) 854-1844

(9) APPENDIX

CLAIMS

1. A method for time stamping a document comprising:
 - a. receiving a time stamp request at an outside agency at a first time, said time stamp request including identifying data associated with said document;
 - b. creating at said outside agency a time stamp receipt based on said identifying data and a time indication; and
 - c. generating at said outside agency a message authentication code based on said time stamp receipt and a secret key;
 - d. transmitting said time stamp receipt and said message authentication code to a designated party;
 - e. receiving a certification request at said outside agency at a second time, said certification request including said time stamp receipt and said message authentication code;
 - f. validating said message authentication code at said outside agency using said secret key; and
 - g. certifying said time stamp receipt at said outside agency using a cryptographic signature scheme if said message authentication code is valid.
2. The time stamping method of claim 1 wherein said identifying data comprises a digital representation of at least a portion of said document.
3. The time stamping method of claim 2 wherein said identifying data comprises a digital sequence derived by application of a deterministic function to at least a portion of said document.

4. The time stamping method of claim 3 wherein said digital sequence is a hash value derived by application of a one-way hashing function to at least a portion of said document.
5. The time stamping method of claim 1 wherein said time stamp receipt includes a copy of at least a portion of said identifying data concatenated with said time indication.
6. The time stamping method of claim 5 wherein said time stamp receipt includes a digital sequence derived from said identifying data concatenated with said time indication.
7. The time stamping method of claim 1 wherein said time stamp request further includes an identification number associated with the requestor.
8. The time stamping method of claim 1 wherein said message authentication code comprises a digital sequence generated by application of a deterministic function to said time stamp receipt and said secret key concatenated together.
9. The time stamping method of claim 6 wherein the step of validating said message authentication code includes recomputing said message authentication code at said outside agency using said received time stamp receipt and said secret key and comparing the recomputed message authentication code to said received message authentication code.

10. The time stamping method of claim 1 wherein the certifying step includes signing said message authentication code using a private signature key controlled by said outside agency.
11. The time stamping method of claim 1 wherein the certifying step includes signing said time stamp receipt using a private signature key controlled by said outside agency.
12. The time stamping method of claim 1 further including the step of storing said secret key in a database at said outside agency.
13. The time stamping method of claim 1 wherein each time stamp receipt includes a sequential record number that is used at said outside agency to look up said secret key in said database.
14. The time stamping method of claim 1 further including the step of transmitting said certified time stamp receipt to said requestor.

15. A method for time stamping a document comprising:
 - a. receiving a time stamp request at an outside agency at a first time, said time stamp request including identifying data associated with said document;
 - b. creating at said outside agency a time stamp receipt based on said identifying data and a time indication;
 - c. generating at said outside agency a message authentication code based on said time stamp receipt and a first secret key;
 - d. encrypting the first secret key with a second secret key to generate a key message;
 - e. generating a second message authentication code based on said first message authentication code and said first secret key using a third secret key;
 - f. transmitting said time stamp receipt, said first message authentication code, said second message authentication code, and said key message to said requestor;
 - g. receiving at said outside agency at a second time a certification request, said certification request including said time stamp receipt, said first message authentication code, said second message authentication code, and said encrypted key message;
 - h. decrypting at said outside agency said encrypted key message to recover said first secret key;
 - i. validating said second message authentication code at said outside agency using said third secret key;
 - j. validating said first message authentication code at said outside agency using said first secret key if said second message authentication code is valid; and
 - k. certifying said time stamp receipt at said outside agency using a cryptographic signature scheme if said first message authentication code is valid.

16. The time stamping method of claim 15 wherein said identifying data comprises a digital representation of at least a portion of said document.
17. The time stamping method of claim 16 wherein said identifying data comprises a digital sequence derived by application of a deterministic function to at least a portion of said document.
18. The time stamping method of claim 17 wherein said digital sequence is a hash value derived by application of a one-way hashing function to at least a portion of said document.
19. The time stamping method of claim 17 wherein said time stamp receipt includes a copy of at least a portion of said identifying data concatenated with said time indication.
20. The time stamping method of claim 19 wherein said time stamp receipt includes a digital sequence derived from said identifying data concatenated with said time indication.
21. The time stamping method of claim 15 wherein said time stamp request further includes an identification number associated with the requestor.
22. The time stamping method of claim 15 wherein said first message authentication code comprises a numeric representation generated by application of a deterministic function to said time stamp receipt and said first secret key concatenated together.

23. The time stamping method of claim 22 wherein said second message authentication code comprises a numeric representation generated by application of a deterministic function to said first message authentication code concatenated with said first and third secret keys.
24. The time stamping method of claim 23 wherein the step of validating said second message authentication code includes recomputing said second message authentication code at said outside agency using said first message authentication code received as part of said certification request, said second secret key and said third secret key, and comparing the recomputed second message authentication code to said received second message authentication code.
25. The time stamping method of claim 24 wherein the step of validating said first message authentication code includes recomputing said first message authentication code at said outside agency using said time stamp receipt received as part of said certification request and said first secret key and comparing the recomputed first message authentication code to said received first message authentication code.
26. The time stamping method of claim 15 wherein the step of certifying said time stamp receipt includes signing said first message authentication code using a private signature key controlled by said outside agency.
27. The time stamping method of claim 15 wherein the step of certifying said time stamp receipt includes signing said time stamp receipt using a private signature key controlled by said outside agency.

28. The time stamping method of claim 15 further including the step of transmitting said certified time stamp receipt to said requestor.

29. A method for time stamping a document comprising:
- a. receiving a time stamp request at an outside agency at a first time, said time stamp request including identifying data associated with said document;
 - b. creating at said outside agency a time stamp receipt based on said identifying data and a time indication; and
 - c. generating at said outside agency a message authentication code based on said time stamp receipt and a secret key; and
 - d. transmitting said time stamp receipt and said message authentication code to said requestor.
30. The time stamping method of claim 29 wherein said identifying data comprises a digital representation of at least a portion of said document.
31. The time stamping method of claim 30 wherein said identifying data comprises a digital sequence derived by application of a deterministic function to at least a portion of said document.
32. The time stamping method of claim 31 wherein said digital sequence is a hash value derived by application of a one-way hashing function to at least a portion of said document.
33. The time stamping method of claim 29 wherein said time stamp receipt includes a copy of at least a portion of said identifying data concatenated with said time indication.

34. The time stamping method of claim 29 wherein said time stamp receipt includes a digital sequence derived from said identifying data concatenated with said time indication.
35. The time stamping method of claim 29 wherein said time stamp request further includes an identification number associated with the requestor.
36. The time stamping method of claim 29 wherein said message authentication code comprises a numeric representation generated by application of a deterministic function to said time stamp receipt and said secret key concatenated together.
37. The time stamping method of claim 29 further including generating a second message authentication code based on said first message authentication code and a second secret key.
38. The time stamping method of claim 37 further including transmitting said second message authentication codes to said requestor.
39. The time stamping method of claim 37 further including the step of encrypting the first secret key to generate an encrypted key.
40. The time stamping method of claim 39 further including transmitting said encrypted key to said requestor.

41. A method for time stamping documents comprising:
 - a. receiving at an outside agency a certification request, said certification request including a time stamp receipt and a message authentication code generated on said time stamp receipt;
 - b. validating said message authentication code at said outside agency using a secret key;
 - c. certifying said time stamp receipt if said message authentication code is valid using a cryptographic signature scheme.
42. The time stamping method of claim 41 wherein the step of certifying said time stamp receipt includes signing said message authentication code at said outside agency using a cryptographic signature scheme.
43. The time stamping method of claim 41 wherein the step of certifying said time stamp record includes signing said time stamp receipt at said outside agency using a cryptographic signature scheme.
44. The time stamping method of claim 41 further including the step of transmitting said certified time stamp receipt to said requestor.
45. The time stamping method of claim 41 wherein certifying said time stamp receipt at said outside agency comprises signing said time stamp receipt with a private signature key.

46. The time stamping method of claim 41 wherein certifying said time stamp receipt at said outside agency comprises signing said message authentication code with a private signature key.
47. The time stamping method of claim 1 wherein certifying said time stamp receipt at said outside agency comprises signing said time stamp receipt with a private signature key.
48. The time stamping method of claim 1 wherein certifying said time stamp receipt at said outside agency comprises signing said message authentication code with a private signature key.
49. The time stamping method of claim 15 wherein certifying said time stamp receipt at said outside agency comprises signing said time stamp receipt with a private signature key.
50. The time stamping method of claim 15 wherein certifying said time stamp receipt at said outside agency comprises signing said message authentication code with a private signature key.